

С-ТЕРРА ЭКРАН-М



Мартышев Андрей

Инженер-консультант

+7 915 459 03 50, доб. 235

amartyshev@s-terra.ru

Архитектура

- Разработана с нуля в 2023 – 2024 г.
- Создавалась под требования ФСТЭК

Сертификация

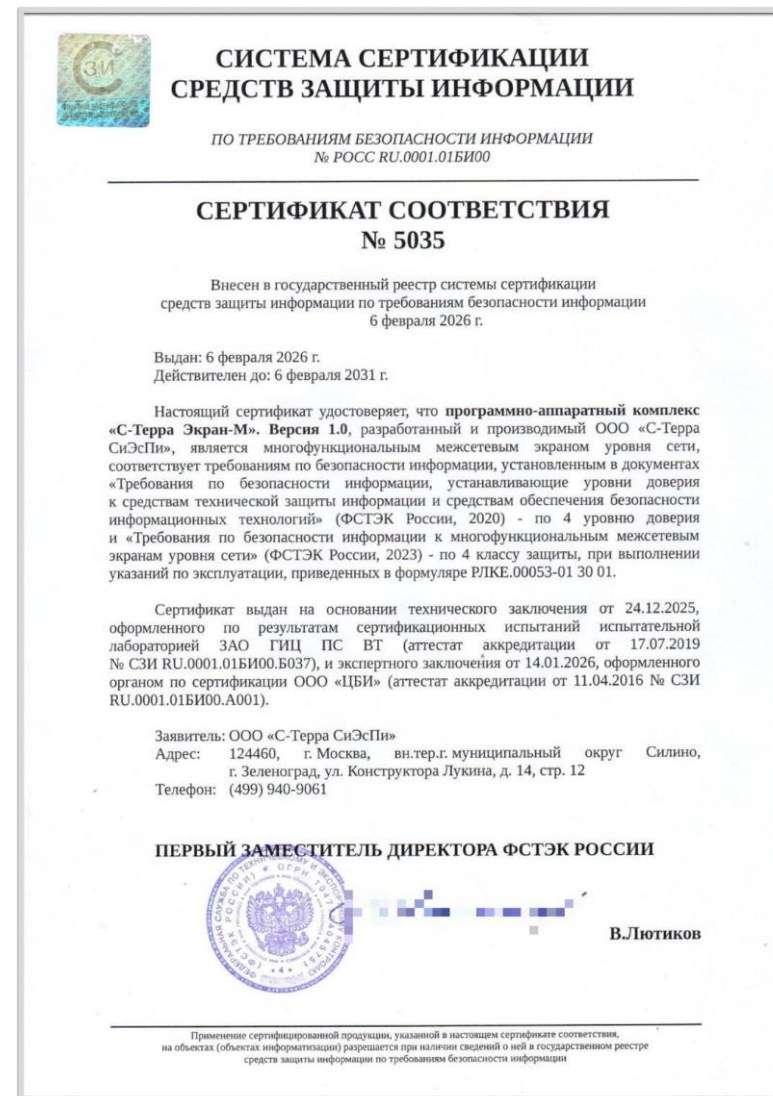
- Российская разработка под ОС Astra Linux
- ФСТЭК по профилю защиты многофункциональных межсетевых экранов уровня сети четвертого класса защиты

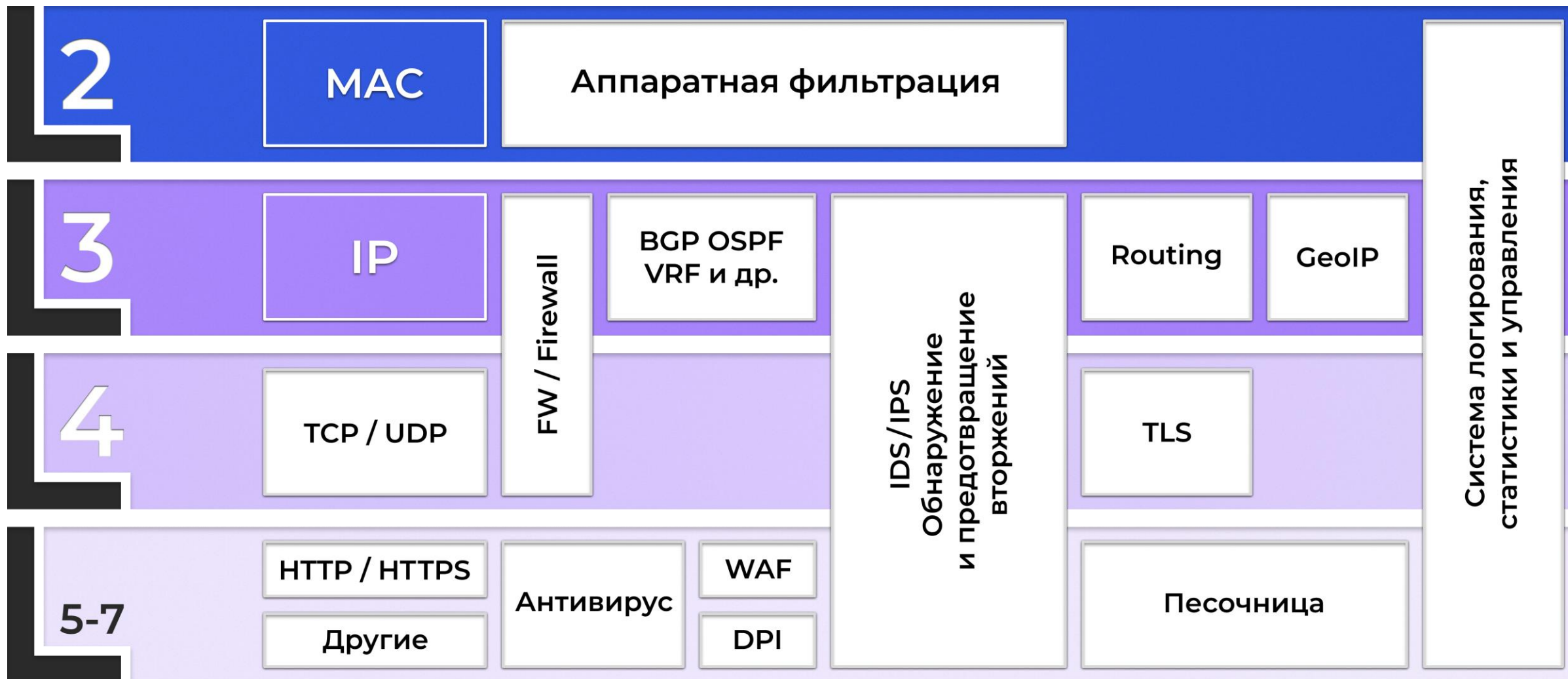
Модульность

- Интеграция с внешними системами
- Гибкое изменение состава модулей


Опыт

- Существующие решения С-Терра
- Экспертиза и компетенции компании с более чем 21 летним опытом работы на рынке ИБ





Новый релиз Экран-М с расширенным функционалом

Экран-М новые релизы в разработке	Защита
	<p data-bbox="1454 501 2219 654">Многофункциональный межсетевой экран уровня сети вместе с ГОСТ-шифрованием</p> <p data-bbox="1429 779 2244 825">Расширенная функциональность</p>

Преимущества подхода

- Многофункциональный межсетевой экран
- Поддержка ГОСТ-шифрования
- Экономия на закупках и обслуживании
- Упрощение архитектуры сети

01	NGFW	04	WAF
02	DPI	05	IDS/IPS
03	SANDBOX	06	ГОСТ VPN

Межсетевой экран с фильтрацией по:

L4

Приложениям

URL

Пользователям, группам и объектам

Расписанию

GeoIP

Расширенные функции:

IPS и IDS

Антивирус

Песочница

WAF

VPN

TLS инспекция

Интеграция с внешней системой DLP

Выбран: eth0 • порт P1

eth0 IN • список 4 (=COMMON P) • правила 9/2

COMMON: Базовая защита (195 366 ON)

COMMON: Базовая защита (copu) (0 ON)

COMMON: Базовая защита (copu) (0 ON)

COMMON: Базовая защита (copu) (0 ON)

COMMON: Базовая защита (copu) (0 ON)

COMMON: Базовая защита (copu) (0 ON)

COMMON: Базовая защита (copu) (0 ON)

COMMON: Базовая защита (copu) (0 ON)

COMMON: Базовая защита (copu) (0 ON)

COMMON: Базовая защита (copu) (0 ON)

eth0 IN: основной (122 179 000 ON)

COMMON: Базовая защита (copu) (0 ON)

COMMON: Базовая защита (copu) (0 ON)

COMMON: Базовая защита (copu) (0 ON)

COMMON: Базовая защита (copu) (0 ON)

COMMON: Базовая защита (copu) (0 ON)

ACL-лист: COMMON: Базовая защита
COMMON (GLOBAL) • правил: 4/4 • Enter — поиск • Esc — закрыть

+ Правило Поиск по №, имени, src/dst, сервису... Только включённые

Выбрано: 0 Все Снять Вкл Вкл Лог+ Лог- ? ? ? ? после # № OK

#	Действие	Сервис	Источник	Назначение	Сработки	Вкл	Лог	Имя
<input type="checkbox"/> #0001	DENY	ANY	192.168.0.0/16	any	12 091	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Deny RFC1918 spoof
<input type="checkbox"/> #0002	PERMIT	UDP/53	any	10.0.0.2	88 012	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Permit DNS to resolver
<input type="checkbox"/> #0003	DENY	TCP/25	10.0.0.0/8	any	430	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Deny SMTP outbound
<input type="checkbox"/> #0004	PERMIT	TCP/443	10.0.0.0/8	any	95 433	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Permit HTTPS outbound

Удобное управление
цепочками правил

Возможность управления
через DRAG & DROP

АВТОМАТИЧЕСКИЕ СКРИПТЫ ПЕРЕНОСА КОНФИГУРАЦИИ

Возможность переноса настроек с оборудования других вендоров (FW + NAT).
Подбор конкретной аппаратной платформы С-Терра осуществляется с учётом требований проекта.

FortiNet



Экран-М (переход)



Check Point



Экран-М (переход)



Песочница получает объекты из различных источников, выполняет проверку и выносит вердикт о вредоносности ПО



- Возможность ручной загрузки объектов с настройкой параметров проверки

- Просмотр журнала анализируемых объектов

Статус проверки	Решение о блокировке	Дата создания ↓	Задание	Вердикт	Источник проверки	Уровень опасности
✓	⚠	2026-03-03T14:08:16+03:00	31ba55e38f0e36371cd3.exe	Опасное ПО	Ручная проверка	10.0 из 10
✓	✓	2026-03-02T23:46:17+03:00	qr ТГ.jpeg	Угроз не обнаружено	Ручная проверка	3.2 из 10
✓	✓	2026-03-02T23:46:12+03:00	qr обычный.png	Угроз не обнаружено	Ручная проверка	2.2 из 10
✓	⚠	2026-03-02T23:36:50+03:00	qr doc.docx	Потенциально Нежелательное ПО	Ручная проверка	5.7 из 10
✓	✓	2026-03-02T23:36:41+03:00	qr ТГ.jpeg	Угроз не обнаружено	Ручная проверка	3.2 из 10

О задании

Добавить сигнатуру в антивирус

Общая информация | Результаты анализа | Анализ угроз

Решение о блокировке **Вердикт** **Уровень опасности** **Статус проверки**

⚠ Зabloкировать **Опасное ПО** **10.0 из 10** ✓ Завершено


Источник для проверки Ручная проверка
Время создания сессии 2026-03-01T23:07:48+03:00
Время окончания сессии 2026-03-01T23:08:25+03:00
Время начала анализа 2026-03-01T23:07:48+03:00
Время завершения анализа 2026-03-01T23:08:17+03:00
Продолжительность анализа 29 сек
Роль Администратор MMЭ
Пользователь sterra_admin
Режим проверки Поведенческий анализ

Типы угроз ▾

Файл
31ba55e38f0e36371cd3.exe

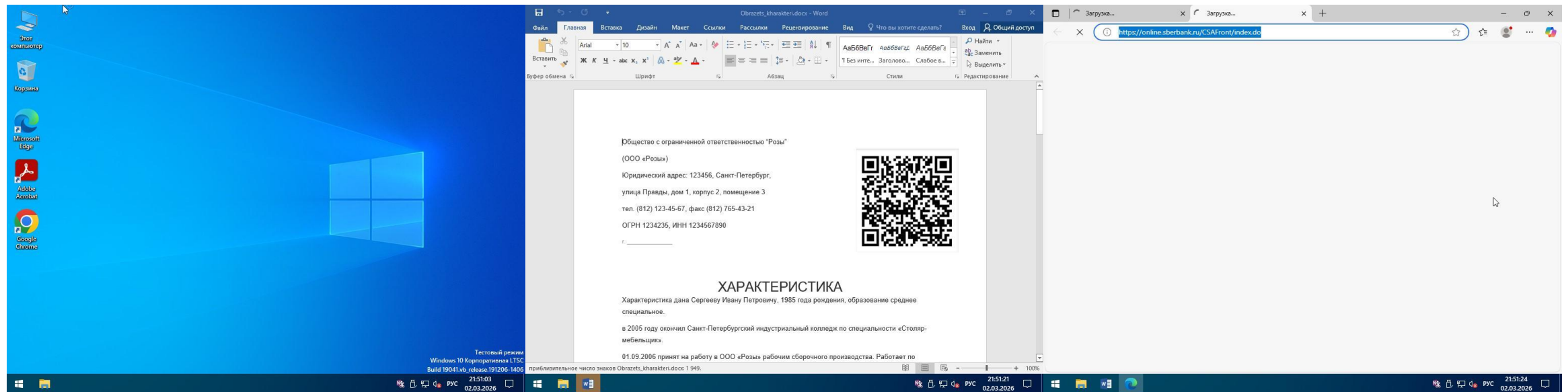
Тип файла	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MIME-тип	application/vnd.microsoft.portable-executable
Формат файла	exe
Размер	213572 bytes
MD5	c9539d1b44440b83c2673361e7225e59
SHA1	1f1e86bb47fa1ef37a2c5dd796e5810b9082eb51
SHA256	31ba55e38f0e36371cd39c8d117617e47261691def9f998262dfe618fca8557

Загрузка файлов:



- Выявленная сетевая активность
- Возможность загрузить pcap файлы и скриншоты анализа
- Создание антивирусных сигнатур на основе вердикта Песочницы
- Обнаруженные сигнатуры Песочницы с маркерами, описывающие поведение файла в изолированной среде

Песочница обнаруживает QR — коды на изображениях или документах, извлекает содержащиеся в них ссылки и проверяет их





Поддержка аппаратных платформ

Поддержка работы на средних и младших платформах ЭКРАН-М



Поддержка отечественных ОС

Установка на Astra Linux, поддержка виртуальных сред с Astra Linux



Динамический обход защитных механизмов

Раскрытие техник анти-песочниц во время анализа



Модули безопасности

Машинное обучение

sterra_admin Администратор ММЭ

Управление **Настройка**

Исключения ^


IP Поиск Q RE* **Добавить**

IP ↑	Направление	Исключенных TCP сессий	Получено	
16.0.165.233	Источник	Включен	4	<input checked="" type="checkbox"/> Изменить Удалить
48.0.101.11	Назначение	Включен	7	<input checked="" type="checkbox"/> Изменить Удалить

Элементов на странице: 5 1 - 2 из 2

События безопасности ^

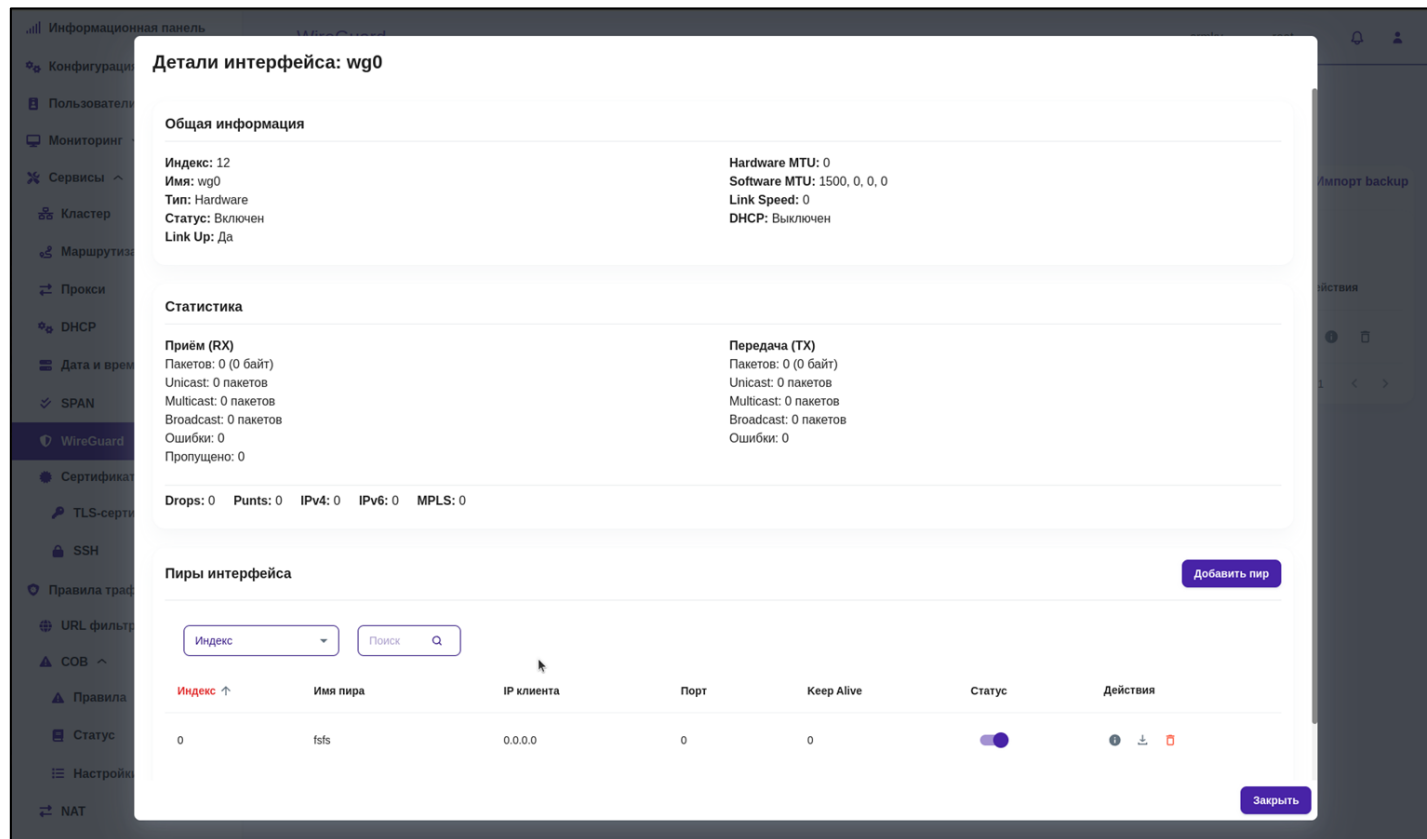
Временная метка (эпоха) Поиск Q RE*

 **Обнаружена атака: PortScan!**

Временная метка (эпоха)	Временная метка (ISO)	Тип атаки	Вероятность атаки	Интерфейс	Источник	Назначение	Порт источника	Порт назначения	Протокол
1770909746	2026-02-12T15:22:26.000Z	PortScan	0.647118	4	192.4.0.99	192.4.0.1	50956	4550	6
1770909746	2026-02-12T15:22:26.000Z	PortScan	0.607341	4	192.4.0.99	192.4.0.1	50956	5800	6
1770909746	2026-02-12T15:22:26.000Z	PortScan	0.62933	4	192.4.0.99	192.4.0.1	50956	49152	6
1770909746	2026-02-12T15:22:26.000Z	PortScan	0.643438	4	192.4.0.99	192.4.0.1	50956	139	6
1770909746	2026-02-12T15:22:26.000Z	PortScan	0.644534	4	192.4.0.99	192.4.0.1	50956	1046	6

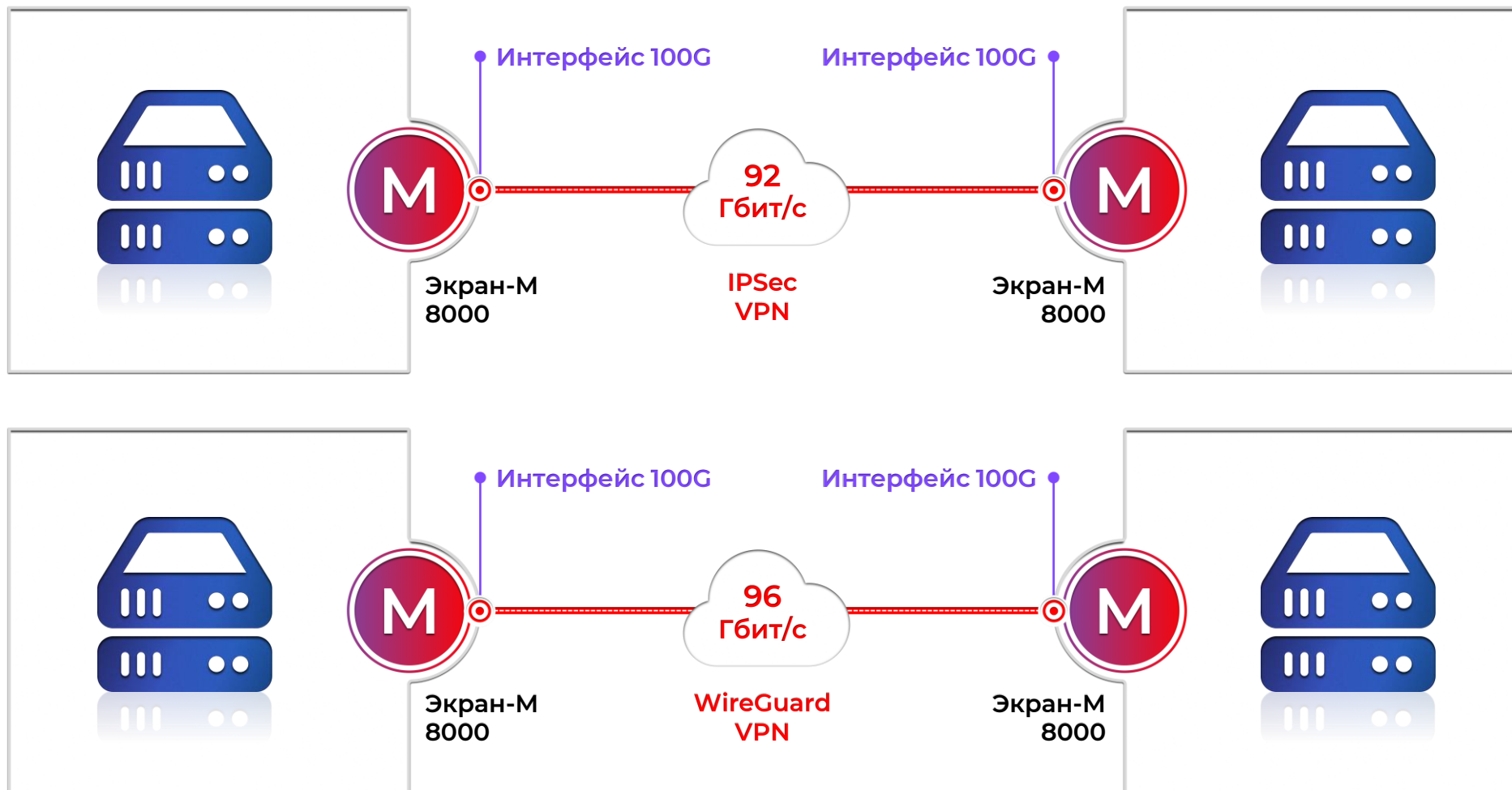
Элементов на странице: 5 1 - 5 из 20

- Журнал исключений IP-адресов
- Оповещение администраторов
- События безопасности
- Поддержка работы на нескольких интерфейсах
- Отображение уровня нормы

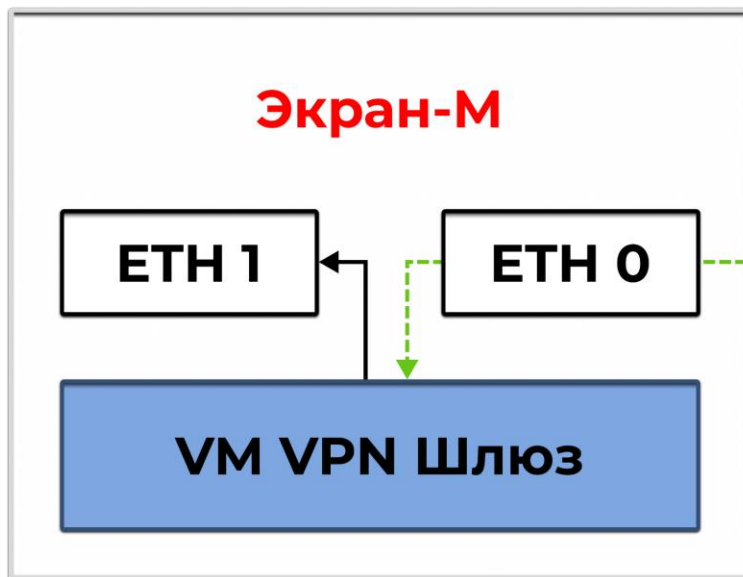


- Реализован как пользовательский плагин
- Шифрует трафик в fast-path без обходов через ядро
- Низкие задержки и высокая пропускная способность ~ равна скорости порта
- Богатая сервис-цепочка: NAT44/NAT66, ACL/ABF (policy-routing), QoS/traffic-policing, VRF/VRF-leak, IDPS, WAF, DPI — всё на одном dataplane

IPSec VPN и WireGuard VPN



Удаленный офис



Центральный офис



Больше, чем вы ждёте

SMTP / NTP-клиент / DHCP (сервер и relay) / PPPoE

- **NAT / PAT**
(трансляция сетевых адресов и портов)
- **VLAN**
(802.1Q)
- **VxLAN**
(Virtual Extensible LAN – виртуализация сети)
- **IPv6**
(NAT, маршрутизация, правила МЭ)
- **SPAN**
(порт зеркалирования)
- **Статическая и динамическая маршрутизация**
(OSPF, BGP)
- **LACP**
(агрегация каналов)
- **Кластеризация**
(отказоустойчивость на базе VRRPv3)

ЭКРАН•М

Информационная панель

Конфигурация

Модули

Система

Подчинённые ПАК

Резервные копии

Пользователи

Мониторинг

Сервисы

Правила трафика

Отчеты и журналы

Внешние системы

Песочница

Антивирус (ClamAV)

Система sterra sterra

Зоны интерфейсов

eth1 Подключите модуль, перетащив его сюда	N/A	Удалить
eth2 Подключите модуль, перетащив его сюда	40 Gbit/s	Удалить
eth3 UNC	40 Gbit/s	Удалить
eth7 Подключите модуль, перетащив его сюда	1 Gbit/s	Удалить
eth6 Подключите модуль, перетащив его сюда	10 Gbit/s	Удалить
eth4 Подключите модуль, перетащив его сюда	1 Gbit/s	Удалить

Перетащите интерфейс сюда

Нераспределённые зоны

LAN / WAN

Экран-М

WAN

eth0 eth5

LAN

eth1 eth2 eth3
eth7 eth6 eth4

eth0 N/A

WAF COB DPI

Удалить

eth5 10 Gbit/s

Подключите модуль, перетащив его сюда

Удалить

Перетащите интерфейс сюда

Нераспределённые интерфейсы

Применение политик безопасности на основе групп и пользователей

Выбор пользователей

- dc=example,dc=com ^
- cn=admin,dc=example,dc=com
- uid=newton,dc=example,dc=com
- uid=einstein,dc=example,dc=com
- uid=tesla,dc=example,dc=com
- uid=galileo,dc=example,dc=com
- uid=euler,dc=example,dc=com
- uid=gauss,dc=example,dc=com
- uid=riemann,dc=example,dc=com
- uid=euclid,dc=example,dc=com
- ou=mathematicians,dc=example,dc=com
- ou=scientists,dc=example,dc=com v
- cn=read-only-admin,dc=example,dc=com
- uid=test,dc=example,dc=com
- ou=chemists,dc=example,dc=com
- uid=curie,dc=example,dc=com
- uid=nobel,dc=example,dc=com

Пользователи сети sterra_admin Администратор ММЭ 🔔 👤

✔ LDAP: соединение успешно

Правила сети **Коннектор** Пользователи сети

Настройка коннектора авторизации пользователя

Сохранение коннектора

Имя коннектора *

Имя хоста * Порт *

Сохранить Очистить

Настройка LDAP

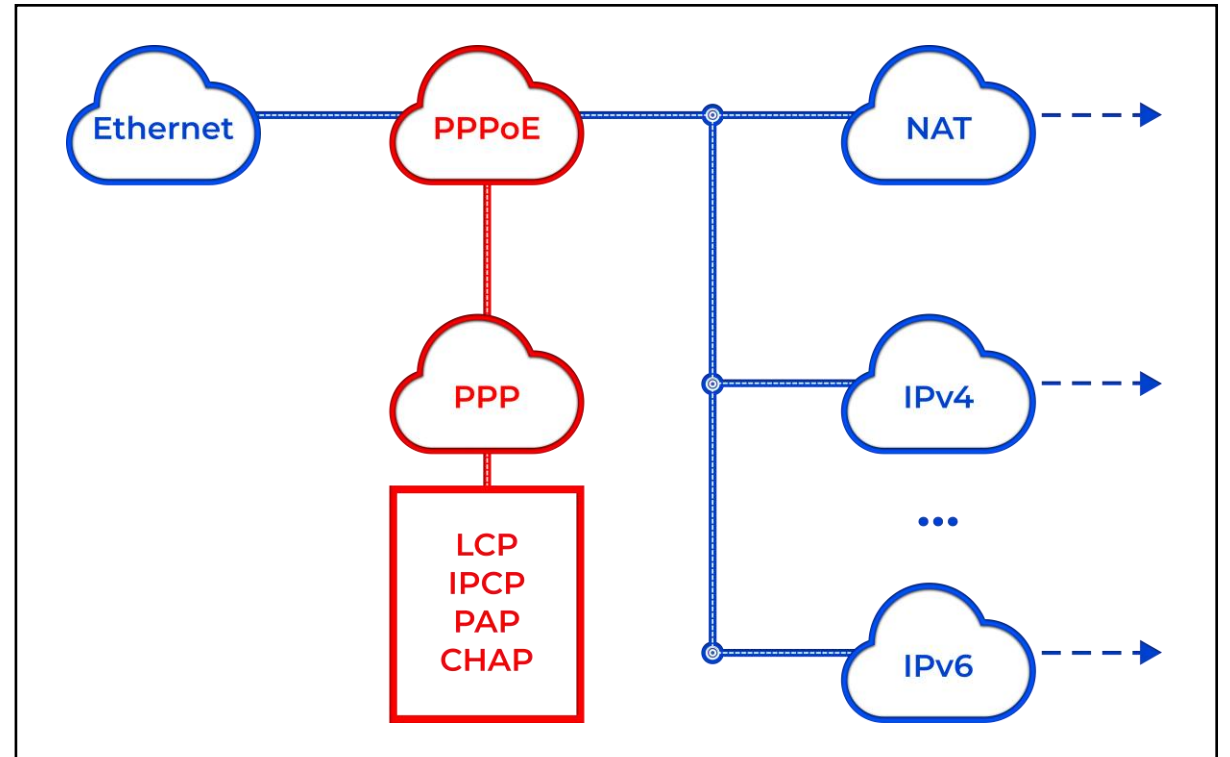
DN *

Фильтр Пароль *

Проверить соединение Показать

Point-to-Point Protocol over Ethernet - прямое подключение к провайдеру

```
show pppoe client session
state:      11111
session_id: 19
sw_if_index: vpp0
LCP id:     7
AUTH id:    0
IPCP id:    3
MRU:        1492
Auth method: CHAP
Magic number: 0x327b23c6
our_ip:     47.1.1.118
peer_ip:    47.1.1.6
dns1:       8.8.8.8
dns2:       8.8.4.4
cookie_len: 20
cookie:     edc08bf80fcf949a660df456aab24d3cd1670000
username:   test
password:   test
provider:   pppoe
-- more -- (2-18/18)
```



Контроль и управление из одного окна

ЭКРАН•М

Информационная панель

Конфигурация

Модули

Система

Подчинённые ПАК

Резервные копии

Пользователи

Учетные записи

Пользователи сети

Обнаруженные устройства

sterra sterra

Подчинённые ПАК

Ваш лицензионный номер для подключения: 1234500890

Название ▼

Поиск
🔍

Добавить группу

Название	Количество	
▼ Без группы	0	
▼ Нижний Новгород	1	
▼ Зеленоград	1	

Элементов на странице: 5 ▼ 1 - 3 из 3 < >

С-Терра Экран-М 8000



С-Терра Экран-М 7000



2024

Протестировано ЦБ РФ

2025

Проверено ФСТЭК РФ

Обработка трафика вынесена за пределы ядра в пользовательское пространство.
Взаимодействие с сетевой картой напрямую

Технологии DPDK и VPP



Пропускная способность в режиме **FW + Stateful + NAT + IPS** для

Экран М 8000 – до 24 Гбит/с

*Согласно тестам

Инфосистемы Джет

Режим работы	Пропускная способность на один порт		Количество правил
	Экран-М 8000	Экран-М 7000	
FW + Stateful	До 96 Гбит/с	До 38 Гбит/с	100 тыс. ACL
FW + IDS / IPS	До 24 Гбит/с	До 12 Гбит/с	100 тыс. ACL + 40 тыс.
FW + IDS / IPS + WAF	До 10 Гбит/с	До 6 Гбит/с	100 тыс. ACL + 60 тыс.
FW + IDS / IPS + DPI + WAF + Антивирус + Песочница	До 5 Гбит/с	До 3.5 Гбит/с	100 тыс. ACL + 150 тыс.

Модификации Экран-М на младших и средних аппаратных платформах

С-Терра Экран-М 100



С-Терра Экран-М 1000



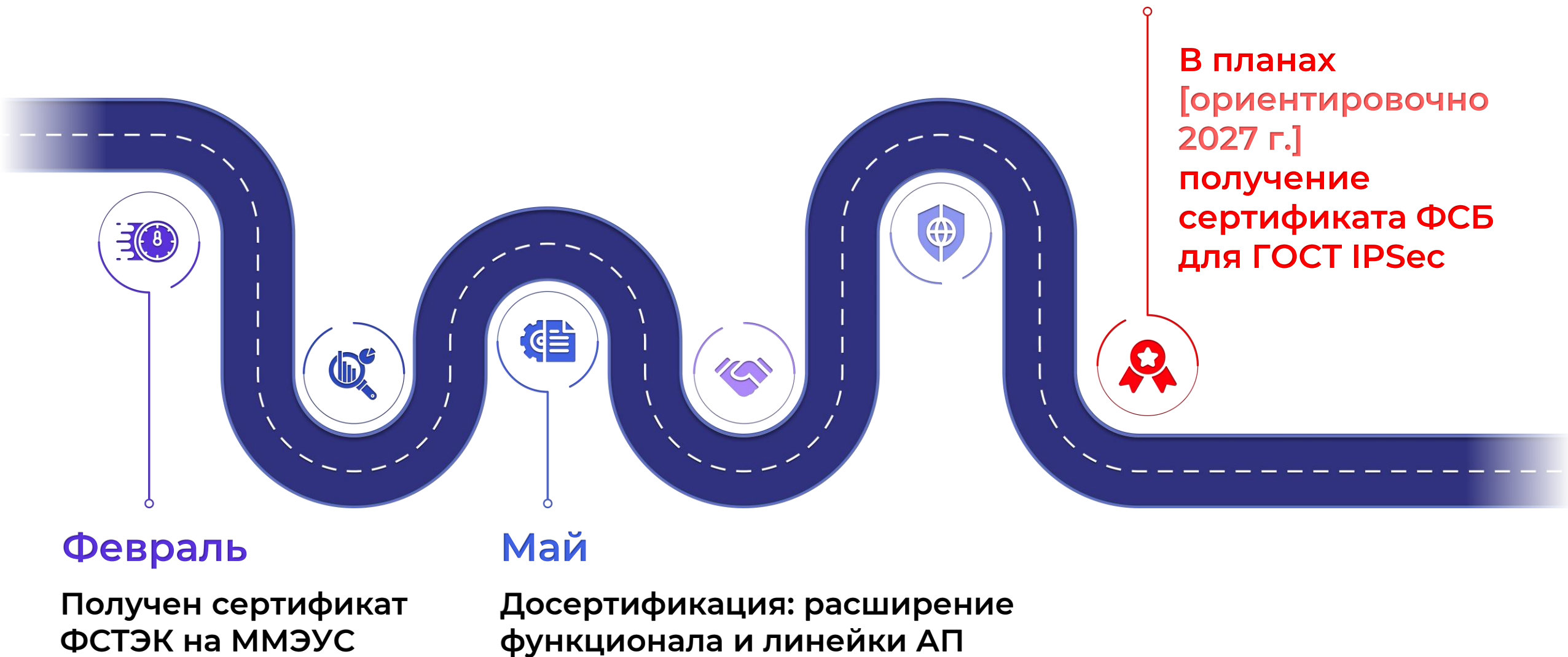
С-Терра Экран-М 3000



С-Терра Экран-М 7000



Вендор	Модель	Скорость L4+L7+IPS	Платформа
С-Терра	100	До 400 Мб/с	СТК-100
С-Терра	1000	До 2 Гб/с	СТК-110
С-Терра	3000 Std	До 5 Гб/с	СТК-120
С-Терра	3000 HE	До 6.5 Гб/с	СТК-120



ОТДЕЛ ПО РАБОТЕ С ПАРТНЁРАМИ



partner@s-terra.ru

Общие вопросы партнёрской политике и развитию бизнеса с «С-Терра»

ОТДЕЛ ПО РАБОТЕ С КЛИЕНТАМИ



sales@s-terra.ru

Получение ценовых условий под проект, размещение заказов и т.д.

ОТДЕЛ ТЕХНИЧЕСКОГО КОНСАЛТИНГА



presale@s-terra.ru

Технические консультации в ходе пресейла

ОТДЕЛ КЛИЕНТСКОГО СЕРВИСА



support@s-terra.ru

Техническая поддержка по купленному оборудованию

СПАСИБО ЗА ВНИМАНИЕ

